

INVERSE-CLOSED ADDITIVE SUBGROUPS OF FIELDS

SANDRO MATTAREI

ABSTRACT. We describe the additive subgroups of fields which are closed with respect to taking inverses. In particular, in characteristic different from two any such subgroup is either a subfield or the kernel of the trace map of a quadratic subextension of the field.

1. INTRODUCTION

The following result of Hua, as stated in [Art57, Theorem 1.15], plays a role in connection with the fundamental theorem of projective geometry (see [Art57, Chapter II, Sections 9 and 10]): an additive map between division rings sending 1 to 1 and inverse elements to inverse elements is either an isomorphism or an antiisomorphism of rings. The first step in the proof is showing that the map preserves the operation $(a, b) \mapsto aba$. This follows from Hua's identity (first mentioned in [Hua49b], but see [Jac68, page 2] or [Jac74, page 89] for the more manageable form given here)

$$(1) \quad a - (a^{-1} + (b^{-1} - a)^{-1})^{-1} = aba,$$

which holds in any associative ring provided all inverses involved are defined, that is, provided a, b and $ab - 1$ are invertible. The rest of the proof (originally given in [Hua49a]) does not use that the map preserves inverses, but rather the product aba . This part of the proof has been later generalized in a number of directions, notably to arbitrary domains by Jacobson and Rickart, see the references given in [Jac68, page 3].

A problem of a similar flavour as Hua's result, but which seems not to have received attention, is a description of the additive subgroups of division rings which contain the inverses of their nonzero elements. In the present note we fill this gap in the commutative case.

For any subset S of a field E we write $S^{-1} = \{s^{-1} \mid 0 \neq s \in E\}$. We call S *inverse-closed* if $S^{-1} \subseteq S$. We prove the following results.

Theorem 1. *Let E be a field of characteristic different from two and let A be a non-trivial inverse-closed additive subgroup of E . Then A is either a subfield of E or the set of elements of trace zero in some quadratic field extension contained in E .*

Conversely, it is plain that the set of elements of trace zero in any quadratic field extension contained in E is inverse-closed.

2000 *Mathematics Subject Classification.* Primary 12E99.

Key words and phrases. field, additive subgroup, inverse.

Partially supported by MIUR-Italy via PRIN 2003018059 "Graded Lie algebras and pro- p -groups: representations, periodicity and derivations".

Theorem 2. *Let E be a field of characteristic two and let A be an inverse-closed additive subgroup of E . Then A is an F^2 -subspace of F for some subfield F of E .*

Conversely, any F^2 -subspace of a subfield F of characteristic two is clearly inverse-closed.

Because of the method of proof employed, based in particular on Hua's identity, it is natural to ask for extensions of Theorems 1 and 2 to division algebras. However, the correct extension is not yet clear to this author from a variety of examples found.

The inversion map in finite fields is of cryptographic interest. For example, inversion in the finite field of 2^8 elements is the nonlinear transformation employed in the S-boxes in the Advanced Encryption Standard (Rijndael) [FIP01]. In view of possible applications, as in [CDVSV], the special case of Theorems 1 and 2 where E is a finite field deserves the following separate mention.

Theorem 3. *Let E be a finite field and let A be a non-trivial inverse-closed additive subgroup of E . Then A is either a subfield of E or the set of elements of trace zero in some quadratic field extension contained in E .*

Note that when E has characteristic two the two alternatives in the conclusion coincide. The finiteness assumption on E allows various proofs of Theorem 3 which differ from that of the general case. For example, one of the advantages of finite fields is that an arbitrary subset can be described by the unique monic polynomial which has the elements of the subset as simple roots. Algebraic properties of the subset often translate into properties of the corresponding polynomial. In particular, here we record a proof of Theorem 3 based on p -polynomials.

I am grateful to A. Caranti for asking the question answered in Theorem 3.

2. PROOFS

Note that an inverse-closed additive subgroup A of E is necessarily a subspace of E over its prime field. This is clear if E has positive characteristic. If E has characteristic zero, then A is a \mathbb{Q} -subspace of E , because $(mn^{-1})a = m(na^{-1})^{-1} \in A$ for $a \in A^*$ and m, n integers with $n \neq 0$.

Lemma 4. *Let A be an inverse-closed additive subgroup of E . Then $a^2b \in A$ for all $a, b \in A$. Furthermore, if E has characteristic different from two, then $abc \in A$ for all $a, b, c \in A$.*

Proof. Hua's identity (1) implies that $aba = a^2b \in A$ for all $a, b \in A$, the degenerate cases where one or more of a, b and $ab - 1$ vanish being obvious. The second assertion follows from the identity $2abc = (a+c)^2b - a^2b - c^2b$. \square

It follows at once by taking $c = 1$ in Lemma 4, that the only inverse-closed additive subgroups containing 1 of a field E of characteristic not two are the subfields of E . According to Theorem 2, this assertion does not extend to arbitrary fields of characteristic two.

Proof of Theorem 1. The inverse-closed subset $K = \{ab \mid a, b \in A\}$ of E is a subring, and hence a subfield, because $ab - cd = a(b - a^{-1}cd) \in K$ and

$(ab)(cd) = (abc)d \in K$ for all $a, b, c, d \in A$ with $a \neq 0$. Choose a nonzero element $a \in A$. Then $Aa^{-1} \subseteq K$, and $Fa \subseteq A$ because of the second assertion of Lemma 4. Hence $A = Fa$, with $a^2 \in K$. We conclude that either A coincides with the subfield K of E , or is the set of elements of trace zero in the quadratic field extension $K(a) = K + Ka$ of E . \square

The following example shows that the subset $\{ab \mid a, b \in A\}$ of E , which we have used in the proof of Theorem 1, need not be a subfield when E has characteristic two. Let $E = \mathbb{F}_2(u_1, u_2, u_3, u_4)$ be a purely transcendental extension of transcendence degree four of the field of two elements \mathbb{F}_2 , and let $A = E^2u_1 + E^2u_2 + E^2u_3 + E^2u_4$. Then $\{ab \mid a, b \in A\} = E^2 + \sum_{i < j} E^2u_iu_j$ is a vector space over E^2 of dimension 7, and hence not a subfield of E .

Proof of Theorem 2. Let R be the subring generated by the squares of the elements of A , and let K be the subfield of E generated by R . The first assertion of Lemma 4 shows inductively that A is an R -submodule of E . Since $ar^{-1} = (a^{-1}r)^{-1} \in A$ for $a \in A$ and $r \in R$ we conclude that A is a K -subspace of E . Finally, if F is the subfield of E generated by A then $K = F^2$ and $A \subseteq F$, as desired. \square

We conclude by giving a proof of Theorem 3 based on p -polynomials. A p -polynomial, over a field of positive characteristic p , is a polynomial all whose monomials have exponents equal to powers of p . A basic property of p -polynomials is that their sets of roots in any field are additive subgroups. We refer to Chapter 3 of [LN83] for an extensive discussion of p -polynomials. We also need the concept of self-reciprocal polynomial. For a polynomial $f(x) = \sum_{i=0}^n a_i x^i$ with $a_0 a_n \neq 0$ we define its *reciprocal* polynomial as $x^n f(1/x) = \sum_{i=0}^n a_{n-i} x^i$. The roots of the reciprocal polynomial are clearly the inverses of the roots of the original polynomial, with corresponding multiplicities. We call *self-reciprocal* a polynomial $f(x) = \sum_{i=0}^n a_i x^i$, with $a_0 a_n \neq 0$, which equals its reciprocal polynomial up to a scalar factor. This clearly implies that $a_n = \pm a_0$. For a polynomial with nonzero constant term and with distinct roots, being self-reciprocal is equivalent to its set of roots being inverse-closed.

Proof of Theorem 3. Let E have order p^f . Then E is the splitting field over \mathbb{F}_p of the polynomial $x^{p^f} - x$. According to Theorems 3.50 and 3.52 of [LN83], the additive subgroups A of E , that is, its \mathbb{F}_p -subspaces, are in a bijection with the monic divisors $f_A(x)$ of $x^{p^f} - x$ which are p -polynomials, given by letting such a polynomial correspond to the set A of its roots. An additive subgroup A of E is inverse-closed if and only if $f_A(x)/x$ is self-reciprocal. Since $f_A(x)$ is a p -polynomial, degree reasons easily imply that it is a binomial, and hence has the form $x^{p^r} - x$ or $x^{p^r} + x$, for some r . In the former case A is the subfield of E of order p^r . In the latter case we may assume that E has characteristic different from two, and hence A is not a subfield. Then the roots in E of the polynomial $x^{p^{2r}} - x$, which include 1, form a subfield of E , of order a divisor of p^{2r} larger than $|A| = p^r$. Hence the roots of the polynomial form a subfield of E of order p^{2r} . The roots of $x^{p^r} + x$ form the kernel of the trace map of this subfield over its subfield of order p^r . \square

REFERENCES

- [Art57] E. Artin, *Geometric algebra*, Interscience Publishers, Inc., New York-London, 1957. MR MR0082463 (18,553e)
- [CDVSV] A. Caranti, F. Dalla Volta, M. Sala, and F. Villani, *Imprimitive permutation groups generated by round functions of AES-like cryptosystems and truncated differential cryptanalysis*, in preparation.
- [FIP01] FIPS Publication 197 (NIST), *Advanced Encryption Standard*, 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [Hua49a] Loo-Keng Hua, *On the automorphisms of a sfield*, Proc. Nat. Acad. Sci. U. S. A. **35** (1949), 386–389. MR MR0029886 (10,675d)
- [Hua49b] ———, *Some properties of a sfield*, Proc. Nat. Acad. Sci. U. S. A. **35** (1949), 533–537. MR MR0031471 (11,155c)
- [Jac68] Nathan Jacobson, *Structure and representations of Jordan algebras*, American Mathematical Society Colloquium Publications, Vol. XXXIX, American Mathematical Society, Providence, R.I., 1968. MR MR0251099 (40 #4330)
- [Jac74] ———, *Basic algebra. I*, W. H. Freeman and Co., San Francisco, Calif., 1974. MR MR0356989 (50 #9457)
- [LN83] Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983, With a foreword by P. M. Cohn. MR **MR746963 (86c:11106)**

E-mail address: `mattarei@science.unitn.it`

URL: `http://www-math.science.unitn.it/~mattarei/`

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI TRENTO, VIA SOMMARIVE 14, I-38050 POVO (TRENTO), ITALY